IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

PATENT APPLICATION

Appellant(s):	**Chandashekhar et al.**	Case:	**Chandashekhar 1-2-1-2-2-2 (LCNT/123980)**
Serial No:	**10/053,801**	Filed:	**01/22/2002**
Examiner:	**Doan, Duyen My**	Group Art Unit:	**2152**
Confirmation #:	**4733**		
Title:	**DYNAMIC VIRTUAL PRIVATE NETWORK SYSTEM AND METHODS**		

MAIL STOP APPEAL BRIEF-PATENTS
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

SIR:

APPEAL BRIEF

Appellants submit this Appeal Brief to the Board of Patent Appeals and Interferences on appeal from the decision of the Examiner of Group Art Unit 2152 mailed April 20, 2007 finally rejecting claims 1, 2 and 4-36.

In the event that an extension of time is required for this appeal brief to be considered timely (**$120** one month extension), and a petition therefor does not otherwise accompany this appeal brief, any necessary extension of time is hereby petitioned for.

The Commissioner is authorized to charge the Appeal Brief fee (**$510**) and any other fees due to make this filing timely and complete (including extension of time fees) to Deposit Account No. 20-0782/LCNT/123980.

Table of Contents

Real Party in Interest

The real party in interest is LUCENT TECHNOLOGIES INC.

Related Appeals and Interferences

Appellants assert that no appeals or interferences are known to Appellants, Appellants' legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of Claims

Claims 1, 2 and 4-36 are pending in the application. Claims 1-36 were originally presented in the application. Claim 3 was canceled. Claims 1, 8-10, 13, 16, 18, 25, 33 and 35 were amended. Claims 1, 2 and 4-36 stand finally rejected as discussed below. The final rejection of claims 1, 2 and 4-36 is appealed.

Status of Amendments

All claim amendments have been entered. Amendments to the claims submitted on June 18, 2007 (in response to the final office action) were entered, as indicated in the Advisory Action of June 26, 2007.

Summary of Claimed Subject Matter

Embodiments of the present invention are generally directed to dynamic management of IP Virtual Private Networks (VPNs) in a manner that enables subscribers to access IP VPN services on an as-needed basis.

In one embodiment, the present invention includes a plurality of internet protocol (IP) services aggregation switches and a dynamic virtual private network (VPN) manager. The IP services aggregation switches enable communications between respective access networks and a core network, and each of the IP services aggregation switches communicates with at least one respective VPN customer user via at least one enhanced integrated access device (EIAD). The dynamic VPN manager provides customer network management and policy server functions, including a user interface enabling remote management of a VPN by a VPN customer user. The VPN has at least one of a defined quality of service (QoS) parameter, a defined security parameter and a corresponding billing rate, where at least one of the QoS parameter and the security parameter is adapted in response to user commands provided to the dynamic VPN manager by the VPN customer user. Additionally, the dynamic VPN manager adapts at least one of the IP services aggregation switches and at least one of the EIADs to provide a bidirectional QoS for at least one IP flow.

In one embodiment, the present invention includes a dynamic virtual private network (VPN) manager that includes an enhanced application portal (EAP), a policy server, and a directory server. The EAP provides a user interface to a VPN customer user, receiving VPN administration commands adapted to configure a VPN. The policy server communicates configuration parameters to network elements providing the VPN, where the network elements include a plurality of internet protocol (IP) services aggregation switches for communicating between respective access networks and a core network and a plurality of enhanced integrated access devices (EIADs) for communicating between VPN customer users and access networks. The network configuration parameters are determined according to VPN administration commands and profiles associated with the VPN administration commands. The directory server stores VPN topology and operational parameters and provides VPN topology and operational parameters to the policy server and the EAP, where the VPN topology and

operational parameters are adapted for being updated by the VPN customer user via the EAP. The VPN manager adapts at least one of the IP services aggregation switches and at least one of the EIADs to provide a bidirectional QoS for at least one IP flow.

In other embodiments, the present invention is a method for performing VPN management activities, or an application programming interface (API) for use by an application to perform VPN management activities. In these embodiments, the steps or functions include receiving, from an authorized VPN customer user, a request to modify a parameter of a virtual private network (VPN) provided in a network comprising a plurality of internet protocol (IP) services aggregation switches for communicating between respective access networks and a core network and a plurality of enhanced integrated access devices (EIADs) for communicating between said VPN customer user and said access networks, retrieving a profile associated with the user request, and providing configuration parameters to at least one of the IP services aggregation switches and at least one of the EIADs in response to the user request and the profile associated with said user request. The at least one of the IP services aggregation switches and the at least one of the EIADs are adapted by the configuration parameter to satisfy the parameter of the VPN, where the parameter of the VPN includes a bidirectional QoS for at least one IP flow.

For the convenience of the Board of Patent Appeals and Interferences, Appellants' independent claims 1, 18, 25 and 35 are presented below with citations to various figures and appropriate citations to at least one portion of the specification for elements of the appealed claims.

Claim 1 positively recites:

1. (previously presented) Apparatus, comprising:

a plurality of internet protocol (IP) services aggregation switches (320) for communicating between respective access networks (30) and a core network (10), each of said IP services aggregation switches (320) communicating with at least one respective VPN customer user (36), wherein said IP services aggregation switches (320) communicate with said at least one VPN customer user (36) via at

least one enhanced integrated access device (EIAD) (310); and (Pg. 9, Lines 3-5, Lines 18-20, Lines 23-27; Pg. 9, Line 29 – Pg. 10, Line 2; Pg. 10, Lines 9-15, Lines 21-24, Lines 27-30)

a dynamic virtual private network (VPN) manager (70), for providing customer network management and policy server functions, including a user interface enabling remote management of a VPN by a VPN customer user (36); (Pg. 8, Lines 2 – 5; Pg. 11, Lines 7-12; Pg. 19, Lines 17-20)

said VPN having at least one of a defined quality of service (QoS) parameter, a defined security parameter and a corresponding billing rate, at least one of said QoS parameter and said security parameter being adapted in response to user commands provided to said dynamic VPN manager (70) by said VPN customer user (36) (Pg. 14, Line 11 – Pg. 15, Line 7; Pg. 26, Lines 27-30);

said dynamic VPN manager (70) adapting at least one of said IP services aggregation switches (320) and at least one of said EIAD (310) to provide a bidirectional QoS for at least one IP flow. (Pg. 8, Lines 2 – 11; Pg. 15, Lines 10 – 14; Pg. 16, Line 15 – Pg. 19, Line 14).

Claim 18 positively recites:

18. (previously presented) A dynamic virtual private network (VPN) manager (70), comprising:

an enhanced application portal (EAP) (71), for providing a user interface to a VPN customer user, and receiving therefrom VPN administration commands adapted to configure a VPN; (Pg. 11, Lines 13-14; Pg. 19, Line 17 – Pg. 20, Line 18)

a policy server (73), for communicating configuration parameters to network elements providing said VPN (Pg. 12, Lines 6-11), said network elements comprising a plurality of internet protocol (IP) services aggregation switches (320) for communicating between respective access networks (30) and a core network (10) and a plurality of enhanced integrated access devices (EIADs) (310) for communicating between VPN customer users (36) and access networks (30), said network configuration parameters determined according to VPN

administration commands and profiles associated with said VPN administration commands (Pg. 9, Lines 3-5, Lines 18-20, Lines 23-27; Pg. 9, Line 29 – Pg. 10, Line 2; Pg. 10, Lines 9-15, Lines 21-24, Lines 27-30); and

a directory server (50), for storing VPN topology and operational parameters and providing said VPN topology and operational parameters to said policy server and said EAP (Pg. 12, Lines 13-15), said VPN topology and operational parameters adapted for being updated by said VPN customer user via said EAP (71) (Pg. 11, Lines 13-17);

said dynamic VPN manager (70) adapting at least one of said IP services aggregation switches (320) and at least one of said EIADs (310) to provide a bidirectional QoS for at least one IP flow (Pg. 8, Lines 2 – 11; Pg. 15, Lines 10 – 14; Pg. 16, Line 15 – Pg. 19, Line 14).

Claim 25 positively recites:

25. (previously presented) A method, comprising:

receiving, from an authorized VPN customer user (36), a request to modify a parameter of a virtual private network (VPN) provided in a network comprising a plurality of internet protocol (IP) services aggregation switches (320) for communicating between respective access networks (30) and a core network (10) and a plurality of enhanced integrated access devices (EIADs) (310) for communicating between said VPN customer user (36) and said access networks (30); (Fig. 4; Pg. 13, Lines 12-22)

retrieving a profile associated with said user request; and (Fig. 4; Pg. 13, Lines 23-25)

providing configuration parameters to at least one of said IP services aggregation switches (320) and at least one of said EIADs (310) in response to said user request and said profile associated with said user request (Fig. 4; Pg. 13, Lines 25-30), said at least one of said IP services aggregation switches (320) and at least one of said EIADs (310) adapted by said configuration parameter to satisfy said parameter of said VPN (Fig. 4; Pg. 13, Lines 25-30), said parameter of

said VPN comprising a bidirectional QoS for at least one IP flow (Pg. 8, Lines 2 – 11; Pg. 15, Lines 10 – 14; Pg. 16, Line 15 – Pg. 19, Line 14).

Claim 35 positively recites:

35. (previously presented) An application programming interface (API) for use by an application to perform VPN management activities (Pg. 8, Lines 12-19), said API performing the functions of:

receiving, from an authorized VPN customer user (36), a request to activate, deactivate, or modify a parameter of a virtual private network (VPN) provided in a network comprising a plurality of internet protocol (IP) services aggregation switches (320) for communicating between respective access networks (30) and a core network (10) and a plurality of enhanced integrated access devices (EIADs) (310) for communicating between said VPN customer user (36) and said access networks (30); (Fig. 4; Pg. 13, Lines 12-22)

retrieving a profile associated with said user request; and (Fig. 4; Pg. 13, Lines 23-25)

providing configuration parameters to at least one of said IP services aggregation switches (320) and at least one of said EIADs (310) in response to said user request or said profile associated with said user request (Fig. 4; Pg. 13, Lines 25-30), said at least one of said IP services aggregation switches (320) and at least one of said EIADs (310) adapted by said configuration parameter to satisfy said parameter of said VPN (Fig. 4; Pg. 13, Lines 25-30), said parameter of said VPN comprising a bidirectional QoS for at least one IP flow (Pg. 8, Lines 2 – 11; Pg. 15, Lines 10 – 14; Pg. 16, Line 15 – Pg. 19, Line 14).

Grounds of Rejection to be Reviewed on Appeal

The Examiner has rejected claims 1-17 under 35 U.S.C. §112, ¶2, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Appellants regards as the invention. Appellants note that the Examiner appears to have inadvertently included claim 3, which has been cancelled, as part of the rejection under 35 U.S.C. §112, ¶2.

The Examiner has rejected claims 1-2, 4-20, 25-30, and 33-36 under 35 U.S.C. §103(a) as being unpatentable over Chanda et al. (U.S. Patent Publication 2002/0095498, hereinafter "Chanda") in view of Pirot et al. (U.S. Patent 6,856,676, hereinafter "Pirot") and further in view of Duffield et al. (U.S. Patent 6,912,232, hereinafter "Duffield").

The Examiner has rejected claims 21-24 and 31-32 under 35 U.S.C. §103(a) as being unpatentable over Chanda, Duffield and Pirot as applied to claims 18 and 25 above and further in view of Forslow (U.S. Patent Publication 2005/0088977, hereinafter "Forslow").

Arguments

35 U.S.C. §112

The Examiner has rejected claims 1-17 under 35 U.S.C. §112, ¶2, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Appellants regard as the invention. Specifically, the Examiner rejected, for lack of antecedent basis, the limitation "said EIADs" in claim 1. Appellants respectfully disagree with the Examiner.

In the response to the Final Office Action dated April 20, 2007, Appellants amended claim 1, in response to the Examiner's rejection under 35 U.S.C. §112, ¶2, from "at least one of said EIADs" to "at least one of said EIAD." In the Advisory Action dated June 26, 2007, the Examiner indicated that this amendment has been entered. Thus, claim 1 currently reads "at least one of said EIAD."

Upon further review, Appellants note that claim 1 includes a limitation that there is "a plurality of internet protocol (IP) services aggregation switches." Appellants further note that claim 1 includes a limitation that each of the plurality of IP services aggregation switches communicates "with at least one respective VPN customer user via at least one enhanced integrated access device (EIAD)" such that there may be considered to be a plurality of VPN customer users and a plurality of EIADs. Thus, there is antecedent basis for a plurality of EIADs.

Appellants respectfully submit that this amendment should be undone. Depending on the outcome of the present appeal, this amendment may be undone by an amendment submitted by Appellants or, alternatively, via Examiner's amendment.

Therefore, the rejection should be withdrawn.

35 U.S.C. §103

Claims 1-2, 4-17

The Examiner has rejected claims 1-2 and 4-17 under 35 U.S.C. §103(a) as being unpatentable over Chanda et al. (U.S. Patent Publication 2002/0095498, hereinafter "Chanda") in view of Pirot et al. (U.S. Patent 6,856,676, hereinafter "Pirot") and further

in view of Duffield et al. (U.S. Patent 6,912,232, hereinafter "Duffield"). The rejection is traversed.

Appellants note that the Examiner referred to "Pancha" in the Final Office Action, dated April 20, 2007; however, "Pancha" was not cited. As Appellants noted in the Response dated June 18, 2007, Appellants presume that Examiner meant "Chanda."

Appellants' claim 1 recites:

> Apparatus, comprising:
> a plurality of internet protocol (IP) services aggregation switches for communicating between respective access networks and a core network, each of said IP services aggregation switches communicating with at least one respective VPN customer user, wherein said IP services aggregation switches communicate with said at least one VPN customer user via at least one enhanced integrated access device (EIAD); and
> a dynamic virtual private network (VPN) manager, for providing customer network management and policy server functions, including a user interface enabling remote management of a VPN by a VPN customer user;
> said VPN having at least one of a defined quality of service (QoS) parameter, a defined security parameter and a corresponding billing rate, at least one of said QoS parameter and said security parameter being adapted in response to user commands provided to said dynamic VPN manager by said VPN customer user;
> said dynamic VPN manager adapting at least one of said IP services aggregation switches and at least one of said EIAD to provide a bidirectional QoS for at least one IP flow.
> [Emphasis added].

In general, Chanda discloses a network system including a plurality of integrated access devices (IADs) assigned to a plurality of clients in a multi-client unit (MCU). As disclosed in Chanda, at least one IAD is assigned to each of the plurality of clients to transmit and receive units of information. The IAD is configured to prioritize data transmissions according to the types of information included in the units of information. An MCU gateway device is assigned to the multi-client unit and coupled to the plurality of IADs to receive or transmit the units of information. The gateway device is configured to prioritize the units of information according to the type of information included in the units of information. (Chanda, Abstract).

Chanda, however, fails to teach or suggest Appellants' claim 1, as a whole. Specifically, Chanda fails to teach or suggest at least the limitation of "said dynamic

VPN manager adapting at least one of said IP services aggregation switches and at least one of said EIAD to provide a bidirectional QoS for at least one IP flow," as claimed in Appellants' claim 1.

Rather, Chanda merely states that IADs may be configured to provide different services to clients communicating via the IADs and gateway devices may be configured to provide different services to clients communicating via the IADs. Although Chanda states that the network system as a whole may allow services to be provided to the clients, such as enabling clients to purchase different amounts of bandwidth according to their needs, and, further, that the IADs and gateway devices may be configured to provide such services to the clients, Chanda is devoid of any teaching or suggestion of adapting both an IAD and a gateway device to provide a service to the client. Rather, Chanda merely describes configuration of the IADs and the gateway device individually.

Furthermore, Chanda is devoid of any teaching or suggestion of a VPN manager configuring IADs or gateway devices to provide such services to the clients. Moreover, Chanda is devoid of any teaching or suggestion that the IADs or gateway devices are adapted to provide a bidirectional QoS, as claimed in Appellants' claim 1. Thus, Chanda fails to teach or suggest at least the limitation of a dynamic VPN manager where "said dynamic VPN manager adapt[s] at least one of said IP services aggregation switches and at least one of said EIAD to provide a bidirectional QoS for at least one IP flow," as claimed in Appellants' claim 1.

In the Final Office Action, dated April 20, 2007, the Examiner cites specific portions of Chanda (namely, Para. 0029 – 0030 and Para. 0055 of Chanda), asserting that the cited portion of Chanda teaches Appellants' limitation of a dynamic VPN manager where "said dynamic VPN manager adapt[s] at least one of said IP services aggregation switches and at least one of said EIAD to provide a bidirectional QoS for at least one IP flow," as claimed in Appellants' claim 1. Appellants respectfully disagree.

Appellants submit that the first portion of Chanda cited by the Examiner (Para. 0029) merely states that the gateway device and IAD may be used by a service provider to provide clients with numerous service features. Appellants submit that a general statement indicating that a gateway and an IAD may be used to provide clients with service features, as taught in Chanda, does not teach or suggest Appellants specific

limitation that at least one IP services aggregation switch and at least one EIAD are adapted, much less that a VPN manager adapts the at least one IP services aggregation switch and the at least one EIAD, or that such devices are adapted to provide bidirectional quality of service for at least one IP flow, as claimed in Appellants' claim 1.

Appellants submit that the second portion of Chanda cited by the Examiner (Para. 0030) merely describes the implementation of the gateway device of Chanda in terms of trunk cards, switch cards, and other line cards which may be included in the gateway device. The cited portion of Chanda is completely devoid of any teaching or suggestion of adapting the gateway device. Furthermore, the cited portion of Chanda is completely devoid of any teaching or suggestion of anything having to do with an IAD. Thus, the cited portion of Chanda simply cannot teach or suggest that a VPN manager adapts the at least one IP services aggregation switch and the at least one EIAD, as claimed in Appellants' claim 1.

Appellants submit that the final portion of Chanda specifically cited by the Examiner (Para. 0055) merely describes arbitration of packets waiting to be transmitted to ensure that higher priority packets are transmitted before lower priority packets. The cited portion of Chanda then provides an example with respect to priority of voice and data packets. Finally, the cited portion of Chanda indicates that the procedure used to transmit packets is similar for both inward-bound data and outward-bound data. While the Examiner has relied upon this portion of Chanda for teaching the "bidirectional quality of service" limitation of Appellants' claim 1, Appellants respectfully note that this portion of Chanda, like the other portions of Chanda cited by the Examiner, also fails to teach or suggest any adaptation of the IAD or gateway device, much less that a VPN manager adapts at least one IP services aggregation switch and at least one EIAD, as claimed in Appellants' claim 1.

Thus, Appellants respectfully submit that Chanda is devoid of any teaching or suggestion of adapting the gateway device or adapting the IAD, much less that either such device is adapted by a dynamic VPN manager or that either such device is adapted by a VPN manager to provide a bidirectional QoS for at least one IP flow. As such, for at least these reasons, Appellants respectfully submit that Chanda fails to teach or suggest at least Appellants' limitation of "said dynamic VPN manager adapting at least one of said

IP services aggregation switches and at least one of said EIAD to provide a bidirectional QoS for at least one IP flow," as claimed in Appellants' claim 1.

Furthermore, Pirot and Duffield, alone or in combination, fail to bridge the substantial gap between Chanda and Appellants' claim 1.

Namely, Pirot and Duffield, alone or in combination with Chanda, fail to teach or suggest at least the limitation of "said dynamic VPN manager adapting at least one of said IP services aggregation switches and at least one of said EIAD to provide a bidirectional QoS for at least one IP flow," as claimed in Appellants' claim 1.

In contrast to Appellants' claim 1, Pirot merely describes a system of controlling and managing voice and data services. The system includes a media gateway controller in communication with a media gateway interface and media gateways. The media gateway controller carries out service logic for a voice or data service according to input received from the media gateways. (Pirot, Abstract). A media gateway controller that carries out service logic based on input that is received from media gateways, as taught in Pirot, does not teach or suggest adapting at least one switch (namely, at least one IP services aggregation switch) and at least one access device (namely, at least one EIAD) to provide a bidirectional QoS for at least one IP flow, much less that the at least one IP services aggregation switch and the at least one EIAD are adapted by a dynamic VPN manager, as claimed in Appellants' claim 1.

Additionally, Pirot discloses a service management subsystem that provides service management tools for managing services, and a service creation subsystem in communication with the service management subsystem for creating the service logic of the services. As taught in Pirot, the service management subsystem includes a service provisioning function for creating and modifying service subscribers and associated profiles, providing service configuration to modify service profiles, providing service activation to launch services, and providing service planning. (Pirot, Col. 7, Line 61 – Col. 8, Line 2). Again, Pirot does not teach or suggest adapting at least one switch (namely, at least one IP services aggregation switch) and at least one access device (namely, at least one EIAD) to provide a bidirectional QoS for at least one IP flow, much less that the at least one IP services aggregation switch and the at least one EIAD are adapted by a dynamic VPN manager, as claimed in Appellants' claim 1.

In contrast to Appellants' claim 1, Duffield merely discloses efficient utilization of network resources in Virtual Private Networks (VPNs). As taught in Duffield, a VPN achieves network resource allocation efficiency by exploiting resource sharing possibilities using multiplexing routing paths between endpoints and dynamic resource allocation techniques that permit real-time resource allocation resizing. Duffield further discloses that, when a VPN is established, routing paths between endpoints of the VPN are optimized for multiplexing opportunities so that resource allocations between nodes along the routing paths within the IP network are reduced to a minimum. (Duffield, Abstract).

Duffield, however, fails to teach or suggest an enhanced IAD, much less adapting an enhanced IAD to provide a bidirectional QoS for at least one IP flow. Similarly, Duffield fails to teach or suggest adapting a switch, much less an IP services aggregation switch, to provide a bidirectional QoS for at least one IP flow. Thus, Duffield must also fail to teach or suggest a VPN manager that adapts at least one switch and at least one access device to provide a bidirectional QoS for at least one IP flow, as claimed in Appellants' claim 1.

Therefore, since Chanda, Pirot, and Duffield each fail to teach or even suggest a VPN manager adapting at least one switch and at least one access device to provide a bidirectional QoS for at least one IP flow, any permissible combination of Chanda, Pirot, and Duffield must also fail to teach or suggest a VPN manager adapting at least one switch and at least one access device to provide a bidirectional QoS for at least one IP flow. Thus, Chanda, Pirot, and Duffield, alone or in any permissible combination, fail to teach or suggest at least the limitation of "said dynamic VPN manager adapting at least one of said IP services aggregation switches and at least one of said EIAD to provide a bidirectional QoS for at least one IP flow," as claimed in Appellants' clam 1.

The test under 35 U.S.C. §103 is not whether an improvement or a use set forth in a patent would have been obvious or non-obvious; rather the test is whether the claimed invention, considered as a whole, would have been obvious. Jones v. Hardy, 110 USPQ 1021, 1024 (Fed. Cir. 1984) (emphasis added). Thus, it is impermissible to focus either on the "gist" or "core" of the invention, Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc., 230 USPQ 416, 420 (Fed. Cir. 1986) (emphasis added). Moreover, the invention as a

whole is not restricted to the specific subject matter claimed, but also embraces its properties and the problem it solves. In re Wright, 6 USPQ 2d 1959, 1961 (Fed. Cir. 1988). Chanda, Pirot, and Duffield, alone or in any permissible combination, fail to teach or suggest Appellants' claim 1, as a whole.

As such, Appellants submit that independent claim 1 is not obvious and fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder. Furthermore, claims 2 and 4-17 depend directly or indirectly from independent claim 1 and recite additional limitations thereof. Accordingly, for at least the same reasons as discussed above, Appellants submit that these dependent claims are also non-obvious and fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Therefore, Appellants respectfully request that the Examiner's rejection be withdrawn.

Claims 18-20

The Examiner has rejected claims 18-20 under 35 U.S.C. §103(a) as being unpatentable over Chanda et al. (U.S. Patent Publication 2002/0095498, hereinafter "Chanda") in view of Pirot et al. (U.S. Patent 6,856,676, hereinafter "Pirot") and further in view of Duffield et al. (U.S. Patent 6,912,232, hereinafter "Duffield"). The rejection is traversed.

The teachings of Chanda, Pirot, and Duffield are discussed hereinabove. For at least the reasons discussed hereinabove with respect to claim 1, Appellants respectfully submit that Chanda, Pirot, and Duffield, alone or in combination, fail to teach or suggest Appellants' claim 18, as a whole. Namely, Chanda, Pirot, and Duffield, alone or in combination, fail to teach or suggest at least the limitation of "said dynamic VPN manager adapting at least one of said IP services aggregation switches and at least one of said EIADs to provide a bidirectional QoS for at least one IP flow," as claimed in Appellants' claim 18.

As such, Appellants submit that independent claim 18 is not obvious and fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder. Furthermore, claims 19-20 depend directly or indirectly from independent claim 18 and recite additional limitations thereof. Accordingly, for at least the same reasons as discussed

above, Appellants submit that these dependent claims are also non-obvious and fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Therefore, Appellants respectfully request that the Examiner's rejection be withdrawn.

Claims 25-30 and 33-34

The Examiner has rejected claims 25-30 and 33-34 under 35 U.S.C. §103(a) as being unpatentable over Chanda et al. (U.S. Patent Publication 2002/0095498, hereinafter "Chanda") in view of Pirot et al. (U.S. Patent 6,856,676, hereinafter "Pirot") and further in view of Duffield et al. (U.S. Patent 6,912,232, hereinafter "Duffield"). The rejection is traversed.

The teachings of Chanda, Pirot, and Duffield are discussed hereinabove. For at least the reasons discussed hereinabove with respect to claim 1, Appellants respectfully submit that Chanda, Pirot, and Duffield, alone or in combination, fail to teach or suggest Appellants' claim 25, as a whole. Namely, Chanda, Pirot, and Duffield, alone or in combination, fail to teach or suggest at least the limitation of "providing configuration parameters to at least one of said IP services aggregation switches and at least one of said EIADs in response to said user request and said profile associated with said user request, said at least one of said IP services aggregation switches and at least one of said EIADs adapted by said configuration parameter to satisfy said parameter of said VPN, said parameter of said VPN comprising a bidirectional QoS for at least one IP flow," as claimed in Appellants' claim 25.

More specifically, as described hereinabove with respect to claim 1, Appellants submit that Chandra, Pirot, and Duffield, alone or in combination, fail to teach or suggest adapting at least one switch and at least one access device to provide a bidirectional QoS for at least one IP flow. As such, although claim 25 does not specifically state that a dynamic VPN manager adapts the at least one IP services aggregation switch and the at least one EIAD, Appellants respectfully submit that such limitation is not required in order to distinguish Appellants' invention from the combination of Chandra, Pirot, and Duffield.

As such, Appellants submit that independent claim 25 is not obvious and fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder. Furthermore, claims 26-30 and 33-34 depend directly or indirectly from independent claim 25 and recite additional limitations thereof. Accordingly, for at least the same reasons as discussed above, Appellants submit that these dependent claims are also non-obvious and fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Therefore, Appellants respectfully request that the Examiner's rejection be withdrawn.

Claims 35-36

The Examiner has rejected claims 35-36 under 35 U.S.C. §103(a) as being unpatentable over Chanda et al. (U.S. Patent Publication 2002/0095498, hereinafter "Chanda") in view of Pirot et al. (U.S. Patent 6,856,676, hereinafter "Pirot") and further in view of Duffield et al. (U.S. Patent 6,912,232, hereinafter "Duffield"). The rejection is traversed.

The teachings of Chanda, Pirot, and Duffield are discussed hereinabove. For at least the reasons discussed hereinabove with respect to claim 25, Appellants respectfully submit that Chanda, Pirot, and Duffield, alone or in combination, fail to teach or suggest Appellants' claim 35, as a whole. Namely, Chanda, Pirot, and Duffield, alone or in combination, fail to teach or suggest at least the limitation of "providing configuration parameters to at least one of said IP services aggregation switches and at least one of said EIADs in response to said user request and said profile associated with said user request, said at least one of said IP services aggregation switches and at least one of said EIADs adapted by said configuration parameter to satisfy said parameter of said VPN, said parameter of said VPN comprising a bidirectional QoS for at least one IP flow," as claimed in Appellants' claim 35.

As such, Appellants submit that independent claim 35 is not obvious and fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder. Furthermore, claim 36 depends directly from independent claim 35 and recites additional limitations thereof. Accordingly, for at least the same reasons as discussed above, Appellants submit

that this dependent claim also is non-obvious and fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

Therefore, Appellants respectfully request that the Examiner's rejection be withdrawn.

Claims 21-24, 31-32

The Examiner has rejected claims 21-24 and 31-32 under 35 U.S.C. §103(a) as being unpatentable over Chanda, Duffield and Pirot as applied to claims 18 and 25 above and further in view of Forslow (U.S. 2005/0088977, hereinafter "Forslow"). Appellants respectfully traverse the rejection.

Claims 21-24 and 31-32 depend, either directly or indirectly, from independent claim 18. For at least the reasons discussed hereinabove, Pirot and Duffield, alone or in combination, fail to teach or suggest Appellants' invention of at least claim 18, as a whole.

Furthermore, Forslow fails to bridge the substantial gap as between Chanda, Duffield, and Pirot and Appellants' claim 18.

In general, Forslow teaches a network-based mobile workgroup system. As taught in Forslow, the network-based mobile workgroup system enables a mobile user to select server resources. (Forslow, Abstract). In particular, as taught in Forslow, the network-based mobile workgroup system provides secure data access to mobile clients. Furthermore, users within a mobile VPN may communicate using intra-domain, inter-domain, or remote-access routing. (Forslow, Pg. 4, Para. 0065, 0067).

Forslow, however, fails to teach or suggest Appellants' invention of at least claims 18, as a whole. Forslow is devoid of any teaching or suggestion of a dynamic VPN manager adapting at least one IP services aggregation switch and at least one EIAD to provide a bidirectional QoS for at least one IP flow, as claimed in Appellants' claim 18.

As such, Chanda, Pirot, Duffield, and Forslow, alone or in any permissible combination, fail to teach or suggest Appellants' claim 18, as a whole. Accordingly, Appellants submit that independent claim 18 is not obvious and fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder. Similarly, independent claims 25 include limitations similar to the limitations of claim 18. Therefore, for at least

the same reasons as discussed with respect to independent claim 18, claim 18 is also not obvious and fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder. Furthermore, claims 21-24 and 31-32 depend, directly or indirectly, from independent claims 18 and 25 and recite additional limitations thereof. Therefore, at least for the same reasons as discussed above, Appellants submit that these dependent claims are also non-obvious and fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Therefore, the rejection should be withdrawn.

Conclusion

Thus, Appellants submit that all of the claims presently in the application are allowable under the provisions of 35 U.S.C. §§112 and 103.

For the reasons advanced above, Appellants respectfully urge that the rejections of claims 1, 2 and 4-36 are improper. Reversal of the rejections of the Final Office Action is respectfully requested.

Respectfully submitted,

Dated: 10/15/07

Eamon J. Wall
Registration No. 39,414
Patterson & Sheridan, L.L.P.
595 Shrewsbury Ave. Suite 100
Shrewsbury, NJ 07702
Telephone: (732) 530-9404
Facsimile: (732) 530-9808
Attorney for Appellant

CLAIMS APPENDIX

LISTING OF CLAIMS:

Please reconsider the claims as follows:

1. (Previously presented) Apparatus, comprising:

a plurality of internet protocol (IP) services aggregation switches for communicating between respective access networks and a core network, each of said IP services aggregation switches communicating with at least one respective VPN customer user, wherein said IP services aggregation switches communicate with said at least one VPN customer user via at least one enhanced integrated access device (EIAD); and

a dynamic virtual private network (VPN) manager, for providing customer network management and policy server functions, including a user interface enabling remote management of a VPN by a VPN customer user;

said VPN having at least one of a defined quality of service (QoS) parameter, a defined security parameter and a corresponding billing rate, at least one of said QoS parameter and said security parameter being adapted in response to user commands provided to said dynamic VPN manager by said VPN customer user;

said dynamic VPN manager adapting at least one of said IP services aggregation switches and at least one of said EIAD to provide a bidirectional QoS for at least one IP flow.

2. (original) The apparatus of claim 1, wherein:

said dynamic VPN manager adapts at least one of said IP services aggregation switches to provide at least one of a guaranteed QoS parameter and a guaranteed security parameter to said VPN.

3. (cancelled)

4. (original) The apparatus of claim 1, wherein:

said dynamic VPN manager adapts at least one of said enhanced integrated access devices (EIAD) to provide at least one of a guaranteed QoS parameter and a guaranteed security parameter to said VPN.

5. (original) The apparatus of claim 1, wherein said QoS parameter comprises at least one of a bandwidth parameter, a jitter parameter and a delay parameter.

6. (original) The apparatus of claim 1, wherein said security parameter comprises at least one of an encryption parameter, an authentication parameter and a filtering parameter.

7. (original) The apparatus of claim 1, wherein said VPN supports at least one of an interactive gaming application and a conferencing application.

8. (previously presented) The apparatus of claim 1, wherein:

said dynamic VPN manager is responsive to a user command to establish an application profile for a VPN, said application profile defining at least one of a QoS parameter, a security parameter and a corresponding billing rate for said VPN during at least one time period;

said dynamic VPN manager adapting said at least one of a QoS parameter and a security parameter of said VPN according to said application profile.

9. (previously presented) The apparatus of claim 1, wherein a command received from the VPN customer user comprises a user selection of one of a plurality of VPNs to join.

10. (previously presented) The apparatus of claim 1, wherein a command received from the VPN customer user comprises a user selection of one of a plurality of applications based on VPNs to join.

11. (original) The apparatus of claim 9, wherein said plurality of VPNs have at least one of respective QoS requirements and security requirements, said QoS and security requirements having corresponding billing rates.

12. (original) The apparatus of claim 10, wherein said plurality of applications have at least one of respective QoS requirements and security requirements, said QoS and security requirements having corresponding billing rates.

13. (previously presented) The apparatus of claim 1, wherein said dynamic VPN manager comprises:

an enhanced application portal (EAP), for providing said user interface to said VPN customer user and receiving therefrom VPN administration commands adapted to configure said VPN;

a policy server, for communicating configuration parameters to network elements providing said VPN, said network configuration parameters determined according to VPN administration commands and profiles associated with said VPN administration commands; and

a directory server, for storing VPN topology and operational parameters and providing said VPN topology and operational parameters to said policy server and said EAP, said VPN topology and operational parameters adapted for being updated by said VPN customer user via said EAP.

14. (original) The apparatus of claim 13, wherein said dynamic VPN manager further comprises:

at least one element management system (EMS) for managing a plurality of network elements forming said VPN.

15. (original) The apparatus of claim 1, wherein said apparatus is included within an internet service provider (ISP) network including said access networks and said core network, said dynamic VPN manager being included within a data center of said ISP.

16. (previously presented) The apparatus of claim 1, wherein said VPN has associated with it a respective name;

said VPN customer user being able to perform at least one of a VPN create, VPN modify, VPN store and VPN delete, command using said VPN name;

said VPN modify command allows said VPN customer user to modify at least one of said VPN's topology, QoS parameter, and security parameter.

17. (original) The apparatus of claim 16, wherein said VPN is retrieved from storage, activated and deactivated using a corresponding VPN name.

18. (previously presented) A dynamic virtual private network (VPN) manager, comprising:

an enhanced application portal (EAP), for providing a user interface to a VPN customer user, and receiving therefrom VPN administration commands adapted to configure a VPN;

a policy server, for communicating configuration parameters to network elements providing said VPN, said network elements comprising a plurality of internet protocol (IP) services aggregation switches for communicating between respective access networks and a core network and a plurality of enhanced integrated access devices (EIADs) for communicating between VPN customer users and access networks, said network configuration parameters determined according to VPN administration commands and profiles associated with said VPN administration commands; and

a directory server, for storing VPN topology and operational parameters and providing said VPN topology and operational parameters to said policy server and said EAP, said VPN topology and operational parameters adapted for being updated by said VPN customer user via said EAP;

said dynamic VPN manager adapting at least one of said IP services aggregation switches and at least one of said EIADs to provide a bidirectional QoS for at least one IP flow.

19. (original) The dynamic VPN manager of claim 18, further comprising:

at least one element management system (EMS) for managing a plurality of network elements forming said VPN.

20. (original) The dynamic VPN manager of claim 18, wherein a managed VPN has associated with it at least one of a defined quality of service (QoS) parameter, a defined security parameter and corresponding billing rate, at least one of said QoS parameter and said security parameter being adapted in response to said VPN administration commands.

21. (original) The dynamic VPN manager of claim 18, wherein:

said dynamic VPN manager is included within a Universal Mobile Telecommunications Services (UMTS) packet transport network, said access networks comprising Gateway Generalized Packet Radio Service support nodes (GGSNs), said user accessing said UMTS packet transport network with a communications device nominally assigned to a home GGSN;

said dynamic VPN manager causing communications with said user communication device to be routed through a GGSN geographically proximate said user communications device.

22. (original) The dynamic VPN manager of claim 21, wherein said determination of geographic location is made during an authentication procedure.

23. (original) The dynamic VPN manager of claim 18, wherein:

said apparatus is included within a CDMA-2000 packet transport network, said access networks comprising home agents, said user accessing said CDMA-2000 packet transport network with a communications device nominally assigned to a home agent;

said dynamic VPN manager causing communications with said user communication device to be routed through a home agent geographically proximate said user communications device.

24. (original) The apparatus of claim 23, wherein said determination of geographic location is made during an authentication procedure.

25. (previously presented) A method, comprising:

receiving, from an authorized VPN customer user, a request to modify a parameter of a virtual private network (VPN) provided in a network comprising a plurality of internet protocol (IP) services aggregation switches for communicating between respective access networks and a core network and a plurality of enhanced integrated access devices (EIADs) for communicating between said VPN customer user and said access networks;

retrieving a profile associated with said user request; and

providing configuration parameters to at least one of said IP services aggregation switches and at least one of said EIADs in response to said user request and said profile associated with said user request, said at least one of said IP services aggregation switches and at least one of said EIADs adapted by said configuration parameter to satisfy said parameter of said VPN, said parameter of said VPN comprising a bidirectional QoS for at least one IP flow.

26. (original) The method of claim 25, wherein said user request is received via an enhanced application portal.

27. (original) The method of claim 25, wherein said parameter to be modified comprises a quality of service (QoS) parameter, said QoS parameter adapting a data flow through a network such that a minimum QoS level is guaranteed to at least a portion of said VPN traversing said network.

28. (original) The method of claim 25, wherein:

said parameter to be modified comprises a security parameter, said security parameter adapting a data flow through a network such that a minimum security level is guaranteed to at least a portion of said VPN traversing said network.

29. (original) The method of claim 27, wherein said QoS parameter comprises at least one of a bandwidth parameter, a jitter parameter, a delay parameter.

30. (original) The method of claim 28, wherein said security parameter comprises at least one of an encryption parameter, an authentication parameter and a filtering parameter.

31. (original) The method of claim 21, wherein said VPN supports at least one application having associated with it at least one of respective QoS requirements and security requirements, said QoS and security requirements having corresponding billing rates.

32. (original) The method of claim 31, wherein said application comprises at least one of an interactive gaming application and a conferencing application.

33. (previously presented) The method of claim 27, wherein said VPN has associated with it a respective name;

said VPN customer user being able to perform at least one of a VPN create, VPN modify, VPN store and VPN delete command using said VPN name;

said VPN modify command allows said VPN customer user to modify at least one of said VPN's topology, QoS parameter, and security parameter.

34. (original) The method of claim 33, wherein said VPN is retrieved from storage, activated and deactivated using a corresponding VPN name.

35. (previously presented) An application programming interface (API) for use by an application to perform VPN management activities, said API performing the functions of:

receiving, from an authorized VPN customer user, a request to activate, deactivate, or modify a parameter of a virtual private network (VPN) provided in a network comprising a plurality of internet protocol (IP) services aggregation switches for communicating between respective access networks and a core network and a plurality of enhanced integrated access devices (EIADs) for communicating between said VPN customer user and said access networks;

retrieving a profile associated with said user request; and

providing configuration parameters to at least one of said IP services aggregation switches and at least one of said EIADs in response to said user request or said profile associated with said user request, said at least one of said IP services aggregation switches and at least one of said EIADs adapted by said configuration parameter to satisfy said parameter of said VPN, said parameter of said VPN comprising a bidirectional QoS for at least one IP flow.

36. (original) The API of claim 35, wherein said application executes on an enhanced application portal.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None